

UNITED STATES DISTRICT COURT  
MIDDLE DISTRICT OF TENNESSEE  
NASHVILLE DIVISION

X \_\_\_\_\_ X  
UNITED STATES OF  
AMERICA,  
Plaintiff,  
v.  
MATTHEW PAUL DEHART,  
Defendant.  
X \_\_\_\_\_ X

3:10-CR-00250

JUDGE TRAUGER

DEFENDANT'S MEMORANDUM OF LAW IN SUPPORT OF HIS MOTION TO  
SUPPRESS

Tor Ekeland (PHV)  
Frederic B. Jennings (PHV)  
Tor Ekeland, P.C.  
195 Plymouth Street  
Brooklyn, NY 11201  
Tel: 718.737.7264  
Fax: 718.504.5417  
tor@torekeland.com  
fred@torekeland.com

*Pro Bono Attorneys for  
Defendant Matthew DeHart*

## TABLE OF CONTENTS

TABLE OF AUTHORITIES .....	iii
INTRODUCTION .....	1
BACKGROUND .....	1
1. The January 2010 Search and Seizure .....	3
2. Arrest and Interrogation in Maine.....	5
3. Mr. DeHart's Emergency Medical Treatment in Maine .....	8
4. Continued Interrogation Without Counsel Present .....	9
PROCEDURAL HISTORY.....	11
LEGAL STANDARD.....	11
ARGUMENTS.....	12
1. Statements Made by Mr. DeHart While in Custody, and Any Physical Evidence Derived from Those Statements, are Inadmissible as They Were Obtained in Violation of Defendant's Fifth Amendment Rights .....	12
2. Incurable Problems With Chain of Custody and Forensic Acquisition Procedures Require Suppression of the Maxtor "BlackArmor" Drive And Gateway Laptop.....	13
3. The Maxtor "BlackArmor" Drive Should Be Suppressed If It Was Decrypted Using Information From, Or Derived From, Statements Made In Violation of Defendant's Fifth Amendment Rights .....	15
4. The January 2010 Search Warrant Is A General Warrant And All Items Seized Under It Should Be Suppressed .....	16
CONCLUSION.....	17

## TABLE OF AUTHORITIES

### **Cases**

<i>Herring v. United States</i> , 555 U.S. 135 (2009).....	12
<i>Miranda v. Arizona</i> , 384 U.S. 436 (1966) .....	12
<i>Nardone v. United States</i> , 308 U.S. 338 (1939) .....	11
<i>Pastorello v. City of New York</i> , 2003 WL 1740606 (S.D.N.Y. Apr. 1, 2003).....	15
<i>Stanford v. Texas</i> , 379 U.S. 476 (1965).....	16, 17
<i>United States v. Blue</i> , 384 U.S. 251 (1966) .....	11
<i>United States v. McFadden</i> , 458 F.2d 440 (6th Cir.1972) .....	13
<i>United States v. Richards</i> , 659 F.3d 527 (6th Cir. 2011).....	16
<i>United States v. Robinson</i> , 367 F. Supp. 1108 (E.D. Tenn. 1973).....	13, 15
<i>United States v. Wright</i> , 343 F.2d 849 (6th Cir. 2003) .....	16

### **Other Authorities**

29 Am.Jur.2d 844, Evidence, § 774 .....	16
Brian Carrier & Eugene H. Spafford, <i>Getting Physical With the Digital Investigation Process</i> , 2 Int'l J. of Digital Evidence 2 (Fall 2003) .....	15
corz.org, <i>checksums explained BLAKE2, SHA1 and MD5 hashing algorithms...</i> , (Sept. 9, 2015 12:46 pm) .....	13
Judy Harrison, <i>Child porn suspect collapses in court</i> , Bangor Daily News, Aug. 11, 2010 .....	9
Mayo Clinic, "Diseases and Conditions: Tachycardia" .....	8
National Institute of Justice Special Report, <i>Forensic Examination of Digital Evidence: A Guide for Law Enforcement</i> , U.S. Dept. of Justice (April 2004).....	15
Tor Project, <i>Tor Hidden Service Protocol</i> .....	1

### **Constitutional Provisions**

U.S. Const. Amend. 4.....	16
---------------------------	----

## **INTRODUCTION**

Defendant Matthew Paul DeHart respectfully submits this Memorandum of Law in Support of his Motion to Suppress.

## **BACKGROUND**

From at least 2003 until his arrest in 2010, Mr. DeHart was affiliated with the Internet activist group “Anonymous”, and was a system administrator for a communal Tor Server used by members of the group.<sup>1</sup> Upon information and belief, during the period of 2008 through 2010 numerous sensitive files appeared on this server that among other things, implicated a federal agency in potential criminal activity against United States citizens, as well as documented apparent malfeasance by American and multinational companies.

Upon information and belief, during this period Mr. DeHart was also part of a drone team at one of the main U.S. Drone Operation Centers in Terre Haute, Indiana, where he was cleared to access to Top Secret Information.<sup>2</sup> Several members of Anonymous were also part of Mr. DeHart’s World of Warcraft Guild during this period, as were, upon information and belief, Alleged Victims # 1 and # 2 that Mr. DeHart is accused of soliciting child pornography from. Alleged Victims # 1 and # 2 lived in Tennessee during the relevant period.

---

<sup>1</sup> A Tor hidden server masks the IP Addresses of those involved with it and provides relatively anonymous browsing. See Tor Project, *Tor Hidden Service Protocol*, available at <https://www.torproject.org/docs/hidden-services.html.en> (last accessed Aug. 31, 2015).

<sup>2</sup> See *United States v. Matthew Paul DeHart*, July 20, 2011 Letter from U.S. Office of Personnel Management to Matthew Dehart at p. 4, 3:10-CR-00250 (M.D. Tenn. (Nashville Div.) Nov. 6, 2012 (ECF #135-4) (Showing Mr. DeHart received provisional Secret clearance, and enlisted with the 181<sup>st</sup> Operations Support Squad).



In January, 2009 the parent of Alleged Victim # 1 contacted the Franklin Police Department. Detective Brett A. Kniss of the Internet Crimes Against Children (“ICAC”) Task Force of Franklin Police Department in Tennessee, took the case.<sup>3</sup> The parent of Alleged Victim # 1, along with the parent of Alleged Victim # 2, were concerned about their sons’ involvement with Defendant Matthew DeHart’s World of Warcraft (“WoW”) guild. Alleged Victim #1 and Alleged Victim #2 were friends at the time. The parent of Alleged Victim #1 had walked by when her son was playing WoW and became upset at the swearing over the game’s live chat (which allows players to talk to each other online) when her son was interacting with someone she later came to believe was Mr. DeHart.<sup>4</sup> Mr. DeHart had allegedly helped Alleged Victim # 2 “Toilet Paper” Alleged Victim’s # 1’s house in the fall of 2008, and this, along with the live chat she overheard of her son playing WoW, and her conversations with Alleged Victim # 2’s mother led her to contact the Franklin Police Department.<sup>5</sup> At some point, the timing of which is unclear from the available discovery, the parent of Alleged Victim #1, allegedly discovered sexually explicit photos on her son’s phone.<sup>6</sup>

On January 9, 2009 Detective Kniss interviewed Alleged Victims # 1 and 2 and examined their cellphones. Alleged Victim # 1’s cellphone was returned to him that day by Detective Kniss.<sup>7</sup> The phone of Alleged Victim # 1 was not maintained, preserved, or

---

<sup>3</sup> Criminal Complaint, Aff. of Brett A. Kniss, at ¶ 4 (ECF # 1); Testimony of Det. Brett A. Kniss, Tr. 60:8 (May 22, 2012) (ECF # 105).

<sup>4</sup> Testimony of Alleged Victim #1’s Mother, Tr. 81: 5-18 (May 22, 2012) (ECF # 105).

<sup>5</sup> Testimony of Alleged Victim #1’s Mother, Tr. 78: 3-5 (May 22, 2012) (ECF # 105).

<sup>6</sup> Criminal Complaint, Aff. of Brett A. Kniss, at ¶ 4 (ECF #1).

<sup>7</sup> *United States v. Matthew Paul DeHart*, Franklin P.D. Evidence Log, 3:10-CR-00250 (M.D. Tenn. (Nashville Div.) Nov. 6, 2012 (ECF #135-14); *See also United States v. Matthew Paul DeHart*, Mot. to Dismiss at pp. 6-7, 3:10-CR-00250 (M.D. Tenn. (Nashville Div.) Sept. 7, 2012) (ECF #123).

forensically analyzed by the Franklin Police Department before being returned to him.<sup>8</sup> Detective Kniss would later testify that he did not recall seeing any pornographic images on the phone of Alleged Victim # 1.<sup>9</sup> On or about February 2009, the Franklin Police Department performed a forensic intake on Alleged Victim # 2's cell phone, which, according to the United States, revealed no evidence of particular significance.<sup>10</sup> After the examination the cell phone was returned to Alleged Victim # 2.<sup>11</sup>

No action was taken by law enforcement against Mr. DeHart in 2009. Upon information and belief, in the fall of 2009 a significant number of files implicating National Security issues appeared on the communal Tor server that Mr. DeHart administered.

#### **1. The January 2010 Search and Seizure**

On or about January 25, 2010, the FBI Office in Evansville, Indiana, in conjunction with the Warrick County Sheriff's Office, executed an Indiana State Search Warrant on Mr. DeHart's residence in Newburgh, Indiana, ostensibly to search for CP.<sup>12</sup> The Affidavit supporting probable cause for the search warrant was not based on personal knowledge and was sworn to by Detective Kurt Pritchett of the Evansville Police Department, Evansville, Indiana.<sup>13</sup> His basis for affirming probable cause was a report on Detective Kniss's January 2009 investigation forwarded to him by Detective Kniss, as

---

<sup>8</sup> Letter from Carrie S. Daughtrey, Assistant United States Attorney, to Defense Counsel Mark C. Scruggs (June 27, 2012) (ECF #135-4); *see also United States v. Matthew Paul DeHart*, Mot. to Dismiss at pp. 6-7, 3:10-CR-00250 (M.D. Tenn. (Nashville Div.) Sept. 7, 2012) (ECF #123).

<sup>9</sup> Testimony of Det. Brett A. Kniss, Tr. 69:22-23 (May 22, 2012) (ECF # 105).

<sup>10</sup> *See* Letter from Carrie S. Daughtrey, Assistant United States Attorney, to Defense Counsel Mark C. Scruggs (June 27, 2012) (ECF #135-4).

<sup>11</sup> *See id.*

<sup>12</sup> *See United States v. Matthew Paul DeHart*, Mot. to Suppress, 1 at ¶ (A), 3:10-CR-00250 (M.D. Tenn. (Nashville Div.) May 21, 2012) (ECF #88-1).

<sup>13</sup> Aff. for Search Warrant (ECF # 88-1).

well as an investigative summary written by Detective Sargent Eric Anderson of the Franklin Police Department.

Incorporated into Detective Kniss's forwarded report are excerpts from two chat logs between one of the alleged victims and unknown screen names. In Detective Kniss's report, these screen names have apparently been altered to read as "DeHart" in one and as "alleged female from Indiana" in another chat log.<sup>14</sup>

During the search, Mr. DeHart's computers and computer related material were seized, as was every other computer in the house, at least 125 digital storage devices and optical media discs and tapes, and one XBOX gaming console and its controllers.<sup>15</sup> Among the items seized were a hardware-encrypted Maxtor 320GB "Black Armor" external hard drive, case serial number listed as 2HC03757, and a Gateway laptop, case serial number listed as 110218873.<sup>16</sup> Mr. DeHart was not arrested, as there was no arrest warrant accompanying the Search Warrant, despite the seriousness of the allegations.<sup>17</sup>

After the search warrant was executed, the seized items appear on the Warrick County Sheriff's Office receipt.<sup>18</sup> It is unclear whether any judge signed the disposition order attached to the search warrant return.<sup>19</sup> No chain of custody logs appear for these seized items prior to 2011, and none have been provided to any defense counsel despite repeated requests from at least July 2011 through August 2015. The defense has only

---

<sup>14</sup> See *id.* at pp. 12-13.

<sup>15</sup> See *id.* at p. 17.

<sup>16</sup> See *id.* at p. 17-18.

<sup>17</sup> *United States v. Matthew Paul DeHart*, Aff. of Bret Kniss at ¶ 11, 3:10-CR-00250 (M.D. Tenn. (Nashville Div.) Aug. 6, 2010) (ECF #1), see also *United States v. Matthew Paul DeHart*, Search Warrant, 3:10-CR-00250 (M.D. Tenn. (Nashville Div.) May 21, 2012) (ECF #88-1).

<sup>18</sup> See *United States v. Matthew Paul DeHart*, Mot. to Suppress, pp. 17-18, 3:10-CR-00250 (M.D. Tenn. (Nashville Div.) May 21, 2012) (ECF #88-1).

<sup>19</sup> See *id.* at p. 19.

been provided federal chain of custody documentation, which do not cover any custody or transfers between the date of seizure and, at the earliest, October 2011.<sup>20</sup>

Forensic reports show that forensic checksums (creation of MD5 and SHA1 hashes) and disk images were made for some of the seized computers, external hard drives, and thumb-drives. However, after being seized on January 25, 2010, forensic checksums were not created for the Gateway laptop's two hard drives until January 29th, and January 31st, 2010.<sup>21</sup> No forensic verification was performed on the Maxtor "Black Armor" encrypted drive until a year and a half later on June 14, 2012.<sup>22</sup> A recent summary report provided to the defense during an on-site evidence review in April, 2015 lists the current location of the Gateway laptop and Maxtor "BlackArmor" encrypted hard drive as "FBI-NT," presumably the Nashville, Tennessee FBI office.<sup>23</sup>

## **2. Arrest and Interrogation in Maine**

Around 8:00 a.m. on August 6th, 2010, at the international border crossing in Calais, Maine, Mr. DeHart crossed the border from Canada into the United States. According to an unclassified FBI 302 report (the "FBI Report"), Mr. DeHart's border crossing set off an alert saying he "was wanted for questioning in an espionage matter." Immigration and Customs Enforcement ("ICE") agents detained Mr. DeHart.<sup>24</sup>

After the ICE agents searched and seized Mr. DeHart's person and belongings, they placed him in a detention cell. Around noon the ICE Agents handed over Mr.

---

<sup>20</sup> See Letter from Kimberly S. Hodde, Partner, Hodde & Associates to S. Carran Daughtrey, Assistant U.S. Attorney, Nashville U.S. Attorney's Office (July 25, 2011), attached as Exhibit B.

<sup>21</sup> See Detective Hill's summary of acquisition for the "DeHart Laptop Computer," attached as Ex. B.

<sup>22</sup> See Defense Team Forensic Report, Maxtor Hard Drive, August 12, 2015, attached as Ex. D.

<sup>23</sup> See Hard Drive List for Forensic Evidence Review, provided to defense counsel on April 23, 2015, attached as Exhibit C.

<sup>24</sup> *United States v. Matthew DeHart*, Unclassified FBI 302 at p. 1, 3:10-CR-00250 (M.D. Tenn. (Nashville Div.) Aug. 26, 2010) (ECF #123-2).



DeHart to FBI Agents from Bangor, Maine. The FBI Agents took him to the border crossing facilities at the International Avenue border crossing in Calais, Maine. The FBI Agents did not promptly take Mr. DeHart to a Federal Magistrate Judge for a detention hearing. Upon arrival at the International Avenue Border Crossing he was placed in another detention cell. The FBI Report states that the FBI began interrogating Mr. DeHart regarding national security matters at approximately 3:15 p.m.<sup>25</sup>

That same afternoon a Criminal Complaint and Arrest Warrant were filed in the Middle District of Tennessee, Nashville Division, alleging a single violation of 18 U.S.C. 2251(a).<sup>26</sup> The charge in the Complaint alleges that “on or about January 1, 2008 and on or about August 31, 2008, in Williamson County, in the Middle District of Tennessee defendant did, knowingly employed, used, persuaded, induced, enticed, and coerced a minor to engage in sexually explicit conduct for the purpose of producing any visual depiction of such conduct, knowing or having reason to know that such visual depictions would be transported in interstate commerce . . . .”<sup>27</sup>

The Supporting Affidavit (“the Affidavit”) to the Complaint is dated August 6, 2010, the same day as Mr. DeHart’s border detention for espionage questioning, and is signed by Brett A. Kniss, Detective, Internet Crimes Against Children Task Force, Franklin Police Department, Tennessee.<sup>28</sup> The Affidavit is based on the above January 9, 2009 investigation, over a year and a half before the filing of the Complaint.<sup>29</sup> It was not

---

<sup>25</sup> See *id.*

<sup>26</sup> *United States v. Matthew DeHart*, Crim. Compl., No. 3:10-CR-00250 (M.D. Tenn. (Nashville Div.) Aug. 6, 2010) (ECF #1).

<sup>27</sup> *Id.*

<sup>28</sup> *United States v. Matthew DeHart*, Aff. of Bret Kniss at p. 8, 3:10-CR-00250 (M.D. Tenn. (Nashville Div.) Aug. 6, 2010) (ECF #1).

<sup>29</sup> *Id.* at ¶¶ 4-5.

until after Mr. DeHart was detained for questioning regarding espionage matters that an arrest warrant in this case was issued. The fax timestamp on the copy of the Complaint faxed from the Middle District of Tennessee to Maine on August 9th, 2010 reads “August 6, 2010 4:00 p.m.,” roughly eight hours after Mr. DeHart was detained.<sup>30</sup>

As with the report attached to the affidavit for the search warrant, Detective Kniss’s allegations are based on chat logs and email addresses that Detective Kniss alleges Mr. DeHart used to solicit sexually explicit material from the minors by pretending to be female girls in Indiana. This is despite the fact that Detective Kniss could not match Mr. DeHart’s Internet Protocol Address (“IP Address”) with the IP Addresses of the alleged females, because logs recording the IP Addresses for the females’ accounts did not exist.<sup>31</sup> It does not appear that Det. Kniss took any further investigative measures to confirm or deny the existence of the alleged females.

Rather than promptly bringing Mr. DeHart before a Federal Magistrate Judge for a detention hearing based on his detention or the Arrest Warrant, at approximately 5:20 p.m. the FBI Agents advised Mr. DeHart that he was being arrested based on the Arrest Warrant.<sup>32</sup>

According to the FBI Report, at approximately 6:00 p.m., two FBI Agents drove Mr. DeHart to the Penobscot County Jail, in Bangor, Maine where he was booked at approximately 7:30 p.m.<sup>33</sup>

---

<sup>30</sup> *United States v. Matthew DeHart*, Crim. Compl., No. 1:10-MJ-00140 (D. Me. Aug. 9, 2010).

<sup>31</sup> *United States v. Matthew Paul DeHart*, Aff. of Bret Kniss at p. 8, 3:10-CR-00250 (M.D. Tenn. (Nashville Div.) Aug. 6, 2010) (ECF #1) at ¶ 10.

<sup>32</sup> *United States v. Matthew DeHart*, Unclassified FBI 302 at p. 3, 3:10-CR-00250 (M.D. Tenn. Aug. 26, 2010) (ECF #123-2).

<sup>33</sup> *Id.* at pp. 4-5.



### 3. Mr. DeHart's Emergency Medical Treatment in Maine

At approximately 1:00 a.m. on August 7th, 2010, hospital records show Mr. DeHart was admitted to the emergency room of the Eastern Maine Medical Center in Bangor, Maine.<sup>34</sup> The E.R. physician's assessment was: 1) Acute Pyschosis; 2) Tachycardia<sup>35</sup>; and 3) eye irritation (possible from having his contact lenses in too long).<sup>36</sup> Additionally, the ER physician noted that Mr. DeHart "verbalize[d] the occasional auditory hallucinations with people calling his name . . ."<sup>37</sup> The ER report stated that Mr. DeHart's symptoms were consistent with "possibl[y] drug-induced psychosis" and that the attending ER physician believed that Mr. DeHart may be experiencing "an acute psychotic break of bipolar disorder or schizophrenia."<sup>38</sup> Urinalysis indicated the presence of Amphetamines.<sup>39</sup> The ER report also stated Mr. DeHart appeared "paranoid and delusional" because he told the physician that FBI agents were accusing him of espionage.<sup>40</sup> Before discharging Mr. DeHart into the care of the "correctional officers," the ER physician discussed "at length that the patient requires psychiatric evaluation while he is incarcerated."<sup>41</sup>

At around 4:30 p.m. on August 7th, 2010 the hospital discharged him into the custody of unknown federal agents who took him back to the Penobscot County Jail

<sup>34</sup> *United States v. Matthew Paul DeHart*, Mem. in Supp. of Mot. to Dismiss, Exs. 1-2, No. 3:10-CR-00250 (M.D. Tenn. (Nashville Div.) Nov. 19, 2014) (ECF #123-1).

<sup>35</sup> Tachycardia "is a faster than normal hear rate at rest." See Mayo Clinic, "Diseases and Conditions: Tachycardia", available at <http://www.mayoclinic.org/diseases-conditions/tachycardia/basics/definition/con-20043012> (last accessed Aug. 10, 2015).

<sup>36</sup> *United States v. Matthew Paul DeHart*, Mem. in Supp. of Mot. to Dismiss, Eastern Maine Medical Center, Emergency Department Record for Matthew DeHart, at p. 3, No. 3:10-CR-00250 (M.D. Tenn. (Nashville Div.) Nov. 19, 2014) (ECF #123-1).

<sup>37</sup> *Id.*

<sup>38</sup> *Id.*

<sup>39</sup> *Id.*

<sup>40</sup> *United States v. Matthew Paul DeHart*, Mem. in Supp. of Mot. to Dismiss, Exs. 1-2, No. 3:10-CR-00250 (M.D. Tenn. (Nashville Div.) Nov. 19, 2014) (ECF #123-1).

<sup>41</sup> *United States v. Matthew Paul DeHart*, Mem. in Supp. of Mot. to Dismiss, Eastern Maine Medical Center, Emergency Department Record for Matthew DeHart, at p. 3, No. 3:10-CR-00250 (M.D. Tenn. (Nashville Div.) Nov. 19, 2014) (ECF #123-1).

where, upon information and belief, he was interrogated by FBI agents over the weekend without counsel present.<sup>42</sup> Upon information and belief, Mr. DeHart repeatedly asked for access to legal counsel throughout the foregoing and was repeatedly denied.

On Monday, August 9, 2010, at approximately 2:00 p.m., Mr. DeHart finally had his initial appearance in front of Federal Magistrate Judge Margaret J. Kravchuk of the Federal District Court for the District of Maine, and she appointed him a Federal Defender. Despite this, upon information and belief, FBI Agents continued to interrogate Mr. DeHart throughout the week without counsel.

#### **4. Continued Interrogation Without Counsel Present**

Upon information and belief, on Monday, August 9, 2010 two Special Agents arrived from the FBI Counterintelligence Office in Washington, D.C. The FBI continued interrogating Mr. DeHart without his counsel present, despite repeated requests by him for his counsel.

On Wednesday, August 11, 2010, at approximately 3:00 p.m., Mr. DeHart appeared in front of Magistrate Judge Kravchuk for a detention hearing on the Criminal Complaint. Judge Kravchuk ordered him detained and committed to the Middle District of Tennessee, Nashville Division, where the Criminal Complaint was pending. At the close of the hearing, according to a local newspaper report, Mr. DeHart collapsed on the courtroom floor.<sup>43</sup> It would be another 9 days before the government began transporting Mr. DeHart to the Middle District of Tennessee.

---

<sup>42</sup> *Id.*

<sup>43</sup> Judy Harrison, *Child porn suspect collapses in court*, Bangor Daily News, Aug. 11, 2010 at <https://www.bangordailynews.com/2010/08/11/news/bangor/child-porn-suspect-collapses-in-court/>

Upon information and belief, over the next nine days, from August 11th to 20th, 2010, the FBI repeatedly interrogated Mr. DeHart without counsel present despite his repeated requests for counsel.

On or about August 19th, 2010, the FBI took Mr. DeHart to a detention facility in New Hampshire. Without his assigned Federal Defender or other counsel present, the FBI induced Mr. DeHart to sign waivers to his right to counsel and to his Miranda rights, and to sign consent forms allowing the FBI to assume, manipulate, and alter Mr. DeHart's Internet accounts including his social online media accounts and email accounts material to this case ("the Accounts").<sup>44</sup> Upon information and belief, at least one of the Accounts appears to have been deleted after the consent forms were signed, as the Defense is unable to access it and the government has not produced any Account data to date despite repeated requests by Mr. DeHart's defense. Among others, Mr. DeHart's ERLOESUNG@GMAIL.COM account appears to have been deleted, and no forensic copy or backup of the account's files or information has been produced, despite repeated requests. Upon information and belief, this account contained exculpatory evidence, including server log files which would have materially aided the defense.<sup>45</sup>

After August 20th, 2010, Mr. DeHart was transferred to a jail in Kentucky to await arraignment and trial on the charges against him in the Middle District of Tennessee, Nashville Division.

---

<sup>44</sup> *United States v. Matthew Paul DeHart*, Mem. in Supp. of Mot. to Dismiss, Exs. 1-2, 3:10-CR-00250 (M.D. Tenn. (Nashville Div.) Nov. 19, 2014) (ECF #123-1 & 123-2).

<sup>45</sup> *United States v. Matthew Paul DeHart*, Aff. of Matthew P. DeHart at p. 5, 3:10-CR-00250 (M.D. Tenn. (Nashville Div.) Nov. 6, 2012) (ECF #135-2)

## **PROCEDURAL HISTORY**

An August 6, 2010 a Criminal Complaint was filed in the Middle District of Tennessee, Nashville Division, charging Mr. DeHart with 1 Count of of violating 18 U.S.C. § 2251(a).<sup>46</sup>

On October 6, 2010, a Grand Jury returned a two count Indictment against Mr. DeHart for production and transportation of Child Pornography.<sup>47</sup> On November 19, 2014, a Grand Jury returned the current four count SI, charging two counts of violation of 18 U.S.C. § 2251(a), one count of violating 18 U.S.C. § 2251(a)(1), and one count of violating 18 U.S.C. 3146(a)(1).<sup>48</sup>

On August 21, 2015, the Government moved to dismiss Count Two of the SI.<sup>49</sup> The Government also filed a Bill of Particulars for Counts One and Two.<sup>50</sup>

Mr. DeHart faces a statutory maximum of seventy years in jail.<sup>51</sup>

## **LEGAL STANDARD**

Evidence must be excluded when it was obtained directly or indirectly in violation of the Defendant's rights under the United States Constitution, federal statutes, or federal rules of procedure. *See, e.g., United States v. Blue*, 384 U.S. 251, 255 (1966). This is true not only for the evidence seized, but for derivative evidence gained as a result of the illegal search or seizure. *See, e.g., Nardone v. United States*, 308 U.S. 338, 340 (1939).

---

<sup>46</sup> *United States v. Matthew Paul DeHart*, Criminal Complaint, 3:10-CR-00250 (M.D. Tenn. (Nashville Div.) Aug. 6, 2010) (ECF #1).

<sup>47</sup> *United States v. Matthew Paul DeHart*, Indictment, 3:10-CR-00250 (M.D. Tenn. (Nashville Div.) Oct. 6, 2010) (ECF #12).

<sup>48</sup> *United States v. Matthew Paul DeHart*, Superseding Indictment, 3:10-CR-00250 (M.D. Tenn. (Nashville Div.) Nov. 19, 2014) (ECF #206).

<sup>49</sup> *United States v. Matthew Paul DeHart*, Gov. Mot. to Dismiss Count Two of Superseding Indictment, 3:10-CR-00250 (M.D. Tenn. (Nashville Div.) Aug. 21, 2015) (ECF #262).

<sup>50</sup> *United States v. Matthew Paul DeHart*, Gov. Bill of Particulars, 3:10-CR-00250 (M.D. Tenn. (Nashville Div.) Aug. 21, 2015) (ECF #263).

<sup>51</sup> *Id.*



The exclusionary rule is a court-created remedy to deter future law enforcement behavior which violates Fourth Amendment. *See Davis v. United States*, 131 S. Ct. 2419, 2427 (2011). When the wrongful law enforcement behavior is “deliberate, reckless, or grossly negligent,” the exclusionary rule should usually be applied as the deterrent effect outweighs the cost of exclusion. *See Herring v. United States*, 555 U.S. 135, 144 (2009).

### **ARGUMENTS**

#### **1. Statements Made by Mr. DeHart While in Custody, and Any Physical Evidence Derived from Those Statements, are Inadmissible as They Were Obtained in Violation of Defendant’s Fifth Amendment Rights**

The instant Mr. DeHart requested counsel, questioning should have ceased and any further questioning required the presence of his appointed attorney. As the Supreme Court said in *Miranda v. Arizona*, 384 U.S. 436, 473-74 (1966), “[A]ny statement taken after the person invokes his privilege cannot be other than the product of compulsion, subtle or otherwise. Further, “[i]f the individual states that he wants an attorney, the interrogation must cease until an attorney is present. At that time, the individual must have an opportunity to confer with the attorney and to have him present during any subsequent questioning.” The waiver of Mr. DeHart’s rights only occurred after his right to counsel was invoked and was done without his assigned Federal Defender or other counsel present. The signed waiver of his rights also allowed the FBI to to assume, manipulate, and alter Mr. DeHart’s Internet accounts including his social online media accounts, and email addresses. The waiver of his rights ineffective as the waiver occurred after the right to counsel was invoked and without the presence of counsel. The proper remedy for a Defendant’s Fifth Amendment rights is the suppression of all testimony and physical evidence derived from the violation.

## **2. Incurable Problems With Chain of Custody and Forensic Acquisition Procedures Require Suppression of the Maxtor “BlackArmor” Drive And Gateway Laptop**

The Maxtor BlackArmor drive, seized during the January 25, 2010 search of the Defendant's family's home, has no forensic verification<sup>52</sup> prior to June 2012, nearly two and a half years after it entered government custody. Additionally, no chain of custody evidence has been provided that can support an assertion of proper acquisition and storage of digital evidence on this drive. Courts have excluded evidence that lacked chain of custody documentation for far shorter periods of time. In *United States v. Robinson*, 367 F. Supp. 1108, 1109 (E.D. Tenn. 1973) the court excluded from evidence a handgun which was unattended for two days without any chain of custody or other intake documents. Further, the court in *United States v. McFadden*, 458 F.2d 440, 441 (6th Cir.1972) held that physical evidence is admissible only when the reasonable probability of misidentification or alteration are eliminated.

Even assuming that digital evidence has the same status as tangible objects despite being far easier to manipulate or damage, the Maxtor BlackArmor drive is inadmissible, unreliable, unverifiable, and should be suppressed. The nearly two-and-a-half-year delay in inventorying the Maxtor BlackArmor drive renders any review for authenticity, credibility, or reliability of the digital evidence difficult if not impossible. Additionally, the drive is hardware-encrypted and no information has been provided by

---

<sup>52</sup> Most commonly, this means MD5 and SHA1 checksums. Both are mathematical functions which return an alphanumeric string uniquely associated with a set of data (such as a disk or disk image, but equally applicable to a file or folder). This numerical “fingerprint” will change if any of that data is altered or deleted. These checksums together serve as a near-certain mathematical verification that data has not been manipulated or damaged between the first checksums’ creation date and a later checksums’ date. See generally [corz.org, checksums explained BLAKE2, SHA1 and MD5 hashing algorithms...](http://corz.org/windows/software/checksum/md5-sha1-blake2-algorithms.php/), (Sept. 9, 2015 12:46 pm), <http://corz.org/windows/software/checksum/md5-sha1-blake2-algorithms.php/> (noting that MD5 has been “cracked” rendering forgery of an MD5 checksum possible).



the government showing the method or means by which it was decrypted. It is possible that Mr. DeHart gave the decryption password to FBI interrogators during the Maine interrogation, in which case his 5<sup>th</sup> Amendment right against self-incrimination is implicated. Without forensic verification from before decryption, there is no way to authenticate this drive. However, without any chain of custody documentation, any forensic verification near to the seizure date, nor any testimony as to the drive image's reliability or decryption, it is impossible to confirm that this drive image has not been misidentified, altered, damaged, or otherwise tampered with.

A similar failure of reliability exists for the Gateway laptop. The delay in that device's forensic intake and verification was four to six days<sup>53</sup>, still plentiful time to alter, misidentify, or tamper with the data therein. Such tampering is conceivable given the extraordinary circumstances of this case and the government espionage investigation into, and its apparent animus against, Mr. DeHart.

Digital evidence is different than standard physical evidence. Digital evidence exists in a far more fragile state and can be easily altered, damaged, or destroyed, intentionally or incidentally, if not carefully acquired and preserved.<sup>54</sup> The act of turning the device off and removing it from the scene may be enough to destroy critical evidence that would otherwise be preserved in read-access memory ("RAM," which stores information on running files and processes) and, depending on the operating system, in other temporary files that may be cleared during the shutdown process. Accidental

---

<sup>53</sup> For unknown reasons, the forensic intake and verification of the Gateway laptop's two physical hard drives took place on different days.

<sup>54</sup> See National Institute of Justice Special Report, *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, U.S. Dept. of Justice (April 2004) at page 1 (12 of PDF), available at: <https://www.ncjrs.gov/pdffiles1/nij/199408.pdf>

deletion or hardware damage in transit also create a major risk of lost data when disk images are not taken on-site. Additionally, digital evidence can be trivially altered by a reasonably competent actor in a matter of minutes. For these reasons and more, digital forensics experts have recommended on-site same-day imaging for over a decade.<sup>55</sup>

To the extent the failures to properly intake, verify, and preserve digital evidence in the present case were contrary to or noncompliant with standard procedures, the evidence should be excluded. Where evidence is left without any identifying marks or verification, no chain of custody, and no other proof to support identification or reliability of the evidence, exclusion is the proper remedy. *See Robinson*, 367 F. Supp. at 1109; *see also* 29 Am.Jur.2d 844, Evidence, § 774.

In the alternative, a negative inference should issue regarding the authenticity of these drives. Even in civil matters, where the duty to preserve evidence is less rigorous, this would be the appropriate remedy for similar failure to reliably preserve hard drive images. *See Pastorello v. City of New York*, 2003 WL 1740606, at \*12 (S.D.N.Y. Apr. 1, 2003). Here, no reliable preservation can be demonstrated, and the failure to preserve identifying and verifying documents is a reckless abuse of discretion by the investigating officers.

**3. The Maxtor “BlackArmor” Drive Should Be Suppressed If It Was Decrypted Using Information From, Or Derived From, Statements Made In Violation of Defendant’s Fifth Amendment Rights**

---

<sup>55</sup> *See* Brian Carrier & Eugene H. Spafford, *Getting Physical With the Digital Investigation Process*, 2 Int’l J. of Digital Evidence 2 (Fall 2003) at p. 17 (describing imaging and verification hash calculation of hard drives while on-scene in an example contraband investigation).

The methods and means of how the Maxtor BlackArmor drive was decrypted are unknown. The Defense has requested this information from the government but has not received an answer beyond summary documents provided in the federal chain of custody. Those documents show that it *was* decrypted, and give some idea of when, but are entirely silent as to *how*. However, if evidence is introduced that suggests the drive was decrypted using a password provided by Mr. DeHart during interrogation by the FBI, or from evidence discovered as a result of that interrogation, it should be suppressed as the interrogation was conducted in violation of Defendant's Fifth Amendment Rights. *See* U.S. Const. Amend. 5.

**4. The January 2010 Search Warrant Is A General Warrant And All Items Seized Under It Should Be Suppressed**

The January 2010 search warrant is also overbroad, and constitutes a “general warrant” of the type prohibited by the 4th Amendment. *See* U.S. Const. Amend. 4; *United States v. Wright*, 343 F.2d 849, 863 (6th Cir. 2003). It fails to provide any objective limiting instruction on what may be seized or searched, in violation of the Defendant's Fourth Amendment right against unreasonable search and seizure. The Sixth Circuit follows the Tenth Circuit rule that “a computer search may be as extensive as reasonably required to locate the items described in the warrant based on probable cause.” *United States v. Richards*, 659 F.3d 527, 538 (6th Cir. 2011) (quoting *United States v. Burgess*, 576 F.3d 1078, 1092 (10th Cir.), cert. denied, — U.S. —, 130 S.Ct. 1028, 175 L.Ed.2d 629 (2009) (citations and internal quotation marks omitted)).

The Supreme Court in *Stanford v. Texas*, 379 U.S. 476 (1965) found a warrant ordering executing officers to search for all “literary material” described as all “books,

records, pamphlets, cards, receipts, lists, memoranda, pictures, recordings and other written instruments concerning state Communist Party and its operations” was a general warrant and violated constitutional requirement that warrants shall particularly describe things to be seized. The January 2010 warrant is a general warrant similar to the warrant in *Stanford v. Texas* because it allows for the seizure of any and all computer hardware and media in the entire DeHart residence without any limiting qualifiers. The appropriate remedy for a general warrant is the suppression of all evidence acquired following the execution of the general warrant. *See id.*

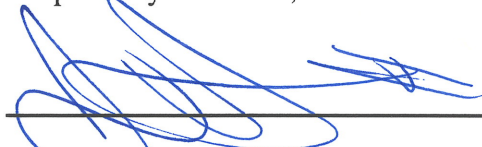
### **CONCLUSION**

For the reasons cited above, the Defendant respectfully requests the Court suppress:

1. All evidence seized during the search executed on or about January 25, 2010;
2. All evidence later discovered or revealed as a direct or indirect result of the January 25, 2010 search, as fruit of the poisonous tree;
3. The Maxtor BlackArmor external hard drive;
4. The Gateway laptop drives;
5. Any evidence discovered or revealed as a result of Mr. DeHart’s interrogation in August, 2010;
6. Any evidence discovered or revealed as a result of the Government’s use, control, or manipulation of Mr. DeHart’s online accounts;
7. Any chain of custody evidence that has not been produced prior to this motion’s filing;
8. All evidence seized or sourced from electronic devices for which a sufficient chain of custody has not been or cannot be produced;

Dated: September 14, 2015

Respectfully submitted,



Frederic B. Jennings (PHV)

Tor Ekeland (PHV)

Tor Ekeland, P.C.

195 Plymouth Street

Brooklyn, NY 11201

Tel: 718.737.7264 ext. 700

Fax: 718.504.5417

Email: tor@torekeland.com

fred@torekeland.com